

## REMARKS

Applicants respectfully request that the above-identified application be reexamined.

Claims 1-42 are pending in this application. An Office Action mailed July 17, 2007 (hereinafter "Office Action"), rejected Claims 1-7, 9-12, 22-25, 27-30, and 40-42 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Application Publication No. 2003/0135613, to Yoshida et al. (hereinafter "Yoshida et al."). Claims 8, 13-21, 26, 31, and 33-38 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Application Publication No. 2004/0249974, to Alkhatib et al. (hereinafter "Alkhatib et al."). Claims 21 and 39 have been amended to correct clerical errors.

Pursuant to 37 C.F.R. § 1.111 and for the reasons set forth below, applicants respectfully request reconsideration and allowance of the pending claims. Prior to discussing in detail why applicants believe that all the claims in this application are allowable, a brief description of the disclosed subject matter and brief descriptions of the teachings of the cited and applied references are provided. The following discussions of the disclosed subject matter and the cited and applied references are not provided to define the scope or interpretation of any of the claims of this application. Instead, these discussions are provided solely to assist the United States Patent and Trademark Office in recognizing the differences between the pending claims and the cited references, and should not be construed as limiting on the disclosed subject matter.

### Disclosed Subject Matter

A method and system for discovering, identifying, and monitoring servers in a heterogeneous network environment are disclosed. Servers in a heterogeneous network are dynamically discovered by first enumerating all of the domains within a network, and second, enumerating all of the known servers in each of the discovered domains. Next, the system acquires and stores additional server contact information necessary to robustly connect to the server. Finally, the system determines the role of the server in a specified domain within the

network. The system continually monitors the connections to the servers and may use the server contact information to connect to the server in case of a network failure.

#### Summary of Yoshida et al.

Yoshida et al. is directed towards a method and system for reducing load on a management server in a load distributed system. (Abstract.) Yoshida et al. discloses, in Figure 1, a load distributed system including a management server 10 provided for managing the network system, an information providing server 20 that stores information to be provided to clients, a network monitoring server 30 that monitors the network, and also acts as an information providing server that stores information to be provided to the clients in the network, a DNS (domain name server) server 4 that manages domain names, an NTS (network time service) server 6 that manages network time, and a client system 40 that receives necessary information from the servers enumerated above. (Yoshida et al., paragraph 0036.) Yoshida et al. states that the server manager 14 manages and monitors the servers 4, 6, 20, and 30. For example, the server manager 14 distributes information among the above-mentioned servers, connects or disconnects the servers to or from the load distributed system, or stops and starts the servers. (Yoshida et al., paragraph 0039.) Yoshida et al. further states that the server list manager 16 selects the servers 4, 6, 20, and 30 to be accessed by a client terminal management server 43 and generates a list of addresses of the selected servers 4, 6, 20, and 30, referred to as a server list. In this configuration, the system may work continuously, even if one of the management servers 10 goes down due to a failure. (Yoshida et al., paragraph 0039.)

In summary, Yoshida et al. is directed to a system and method for reducing load on a management system with a pre-determined network configuration.

#### Summary of Alkhatib et al.

Alkhatib et al. is directed to a secure communication system that allows local and remote devices to communicate from any location via an Internet connection. (Alkhatib et al., paragraph 0005.) Alkhatib et al. describes a system and method that allows local and remote

devices to communicate from various locations using a virtual subnet with a virtual address realm. The virtual address realm allows two or more users to communicate securely via a public network, regardless of whether the users are connected to a public or a private network. The virtual address realm uses virtual addresses to identify the devices on the virtual subnet. Although the devices may be in different physical subnets, from the perspective of applications, the devices of the virtual subnet appear to be in one local subnet. (Alkhatib et al., paragraph 0028.)

In summary, Alkhatib et al. is directed to a communication system for allowing remote and local devices to communicate securely via public networks.

Rejection of Claims 1-6, 7, 9-12, 22-25, 27-30, and 40-42 Under 35 U.S.C. § 102(e)

As indicated above, Claims 1-6, 7, 9-12, 22-25, 27-30, and 40-42 were rejected under 35 U.S.C. § 102(e) as being anticipated by Yoshida et al. Applicants respectfully disagree for the reasons set forth below.

Independent Claim 1 recites, in its entirety:

1. A system for discovering and identifying a server, the system comprising:
  - a network comprising at least one domain, wherein at least one domain comprises at least one server; and
  - a communication device comprising:
    - a server monitoring unit operable for:
      - dynamically discovering** at least one server on the network;
      - monitoring at least one server on the network; and
      - determining information** associated with the monitored server, wherein the **information is used to connect to the monitored server after a network failure** situation; and
    - a potential server storage unit operable for:
      - storing the information associated with the monitored server. (Emphasis added.)

Yoshida et al. does not disclose dynamically discovering at least one server on the network. Those skilled in the art will appreciate that "discovery" is a term of art indicating the finding of unknown servers in a network. The process of discovery is generally carried out by

sending discovery packets over a network and analyzing the responses returned by various servers to identify what servers may exist on the network.

Yoshida et al. discloses a network with a known configuration. Figure 1 of Yoshida et al. clearly shows all the servers and computing components included in the Yoshida et al. network. Yoshida et al.'s description of Figure 1 clearly enumerates all the servers included in the network and their respective roles. (Yoshida et al., paragraph 0036.) Because all servers are predetermined and their relationships are established, Yoshida et al. has no need for a discovery process and does not teach, disclose, or even remotely suggest such a process.

Yoshida et al. also does not teach, disclose, or suggest determining information associated with a monitored server. Yoshida et al. states that a server manager 14 manages and monitors the servers 4, 6, 20, and 30. Yoshida et al. further states that the server manager 14, for example, distributes information among the servers, connects or disconnects the servers, etc. (Yoshida et al., paragraph 0039.) Distributing information is not the same as determining information. To distribute information, the information must be pre-existing. This is in contrast to determining information, which implies that the information is unknown and is determined on some basis. More specifically, Yoshida et al. discloses that the server list manager 16 selects the servers 4, 6, 20, and 30 to be accessed by the client's terminal management server 43 and generates a list of addresses of the selected servers 4, 6, 20, and 30. Again, generating a list of addresses of the selected servers requires the addresses to be known. This is in contrast to determining information associated with a monitored server, wherein the information is used to connect to the monitored server, as recited in Claim 1.

Yoshida et al. also does not disclose using such determined information, i.e., information associated with the monitored server, to connect to the monitored server after a network failure, as recited in Claim 1. Yoshida et al. discloses that the described configuration allows the system to work continuously, even if one of the management servers 10 goes down due to a failure. (Yoshida et al., paragraph 0039.) Those skilled in the art will appreciate that network failure is

not the same as server failure. Network failure causes a network path to be unavailable for transmitting data. This is in contrast to a server failure, where the services of the particular server are not available due to the failure. The distinction between a server failure and a network failure is further emphasized in the Claim 1 language that reads "... the information is used to connect to the monitored server after a network failure situation." (Emphasis added.) The claim language clearly indicates that the determined information is used to connect to the monitored server after a network failure. Therefore, Claim 1 is submitted to be allowable for at least the reasons discussed above.

Claims 2-6 depend from Claim 1 and are submitted to be allowable for at least the same reasons discussed above with respect to Claim 1.

Claim 7 recites substantially similar features to Claim 1 and is submitted to be allowable for at least the same reasons discussed above with respect to Claim 1.

Claims 8-21 depend from Claim 7 and are submitted to be allowable for at least the same reasons discussed above with respect to Claim 7. Additionally, other features are recited in the claims depending from Claim 7 that are not disclosed by Yoshida et al. For example, Claim 9 recites: "generating a first list of enumerated domains through domain trust discovery; generating a second list of enumerated domains through directory partitions discovery." Yoshida et al. does not disclose generating a list of enumerated domains through either domain trust discovery or directory partitions discovery. Therefore, Claim 9 is submitted to be allowable for these additional reasons.

Claim 25 recites substantially similar features to Claim 1 and 7 discussed above and is submitted to be allowable for at least the same reasons as discussed above with respect to Claim 1.

Claims 26-39 depend from Claim 25 and are submitted to be allowable for at least the same reasons discussed above with respect to Claim 25.

Claim 22-24 and 40-42

Claim 22 recites, in its entirety:

22. A method for identifying a server in a network, the method comprising:  
designating a remote computer for determining a **server role** for the remote computer;  
**selecting a role inquiry from a set of role inquiries;**  
**querying the remote computer with the role inquiry;**  
receiving a response to the role inquiry from the remote computer;  
and  
attempting to **determine a server role** of the remote computer **from the response**. (Emphasis added.)

Yoshida et al. does not disclose determining a server role for a remote computer. Yoshida et al. discloses a client terminal management server 43 that regularly sends inquiries to a network monitoring server 30. This inquiry is used to monitor the client terminal management server 43. The network monitoring server 30 knows in advance which client terminal management server 43 will access the network monitoring server 30. When the client terminal management server 43 fails to send an inquiry for a predetermined time, that client terminal management server 43 is thought to have failed. (Yoshida et al., paragraph 0070.) Yoshida et al. clearly discloses that the relationship between various servers, such as servers 43 and server 30 are known in advance. Therefore, the roles of the servers are not determined by Yoshida et al. Rather, they are predetermined and are already known by other servers. Yoshida et al. discloses that if a server 43 fails to send an inquiry for a predetermined time, that client terminal management server 43 is thought to have failed. Therefore, Yoshida et al. discloses a determination of a failure of a server, in contrast to determination of the role of the server.

Furthermore, Yoshida et al. does not disclose selecting a role inquiry from a set of role inquiries. Nor does Yoshida et al. disclose querying the remote computer with the role inquiry. Additionally, Yoshida et al. does not disclose receiving a response to the role inquiry from the remote computer. Finally, Yoshida et al. does not disclose attempting to determine a server role

of the remote computer from the response. Therefore, independent Claim 22 is submitted to be allowable for at least the reasons discussed above.

Claims 23-24 depend from Claim 22 and are submitted to be allowable for at least the same reasons as discussed above with respect to Claim 22.

Independent Claim 40 recites substantially the same features as Claim 22 and is submitted to be allowable for at least the same reasons as discussed above with respect to Claim 22. Claims 41 and 42 depend from Claim 40 and are submitted to be allowable for at least the same reasons discussed above with respect to Claim 40.

Rejection of Claims 8, 13-21, 26, 31, and 33-38 Under 35 U.S.C. § 103(a)

As indicated above, Claims 8, 13-21, 26, 31, and 33-38 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Alkhatib et al. Applicants respectfully disagree for the reasons set forth below.

As noted above, Claims 8 and 13-21 and Claims 26, 31, and 33-38 depend from independent Claims 7 and 25, respectively, and are submitted to be allowable for at least the reasons discussed above. Alkhatib et al. fails to supply the teachings missing from Yoshida et al. Alkhatib et al. is directed toward a private virtual network for secure communication between devices coupled with different subnets. (Alkhatib et al., paragraph 0028.) Alkhatib et al. does not disclose dynamically discovering at least one server on a network, receiving a name of the at least one server on the network, determining whether the network is functioning properly, and connecting to the at least one server, if the network is not functioning properly, as recited in Claim 7 and, by dependency, Claim 8. Therefore, Claims 8, 13-21, 26, 31, and 33-38 are submitted to be allowable for these reasons.

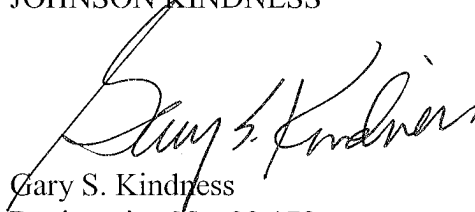
Additionally, other features are recited in the above-mentioned claims that are submitted to be allowable for additional reasons. For example, Claim 27 recites substantially the same features as Claim 9 and is submitted to be allowable for those additional reasons.

### CONCLUSION

Applicants respectfully submit that all the claims in this application are clearly allowable in view of the disclosures of Yoshida et al. and Alkhatib et al. Therefore, applicants respectfully request that this application be reexamined, all of the claims remaining in this application be allowed, and this application be passed to issue. If the Examiner has any questions, the Examiner is invited to contact the applicants' attorney at the number set forth below.

Respectfully submitted,

CHRISTENSEN O'CONNOR  
JOHNSON KINDNESS<sup>PLLC</sup>



Gary S. Kindress  
Registration No. 22,178  
Direct Dial No. 206.695.1702

GSK/FXM:tmn

LAW OFFICES OF  
CHRISTENSEN O'CONNOR JOHNSON KINDNESS<sup>PLLC</sup>  
1420 Fifth Avenue, Suite 2800  
Seattle, Washington 98101  
206.682.8100